created by
e-skills uk

In partnership with:

The National B2B Centre
Helping growing businesses make smart e-business decisions

Business IT Guide

Enables businesses to make the right IT decisions

e-Security Pack for businesses

http://www.businessitguide.com

Introduction

This pack includes a series of guides from the Business IT Guide which will give you background knowledge on key aspects of e-security, and point you in the direction of further security products and advice. Areas covered range from securing important data in the office and on the move, to protecting your computers from viruses and malware. Finally, two of the Guide’s top IT security experts give their views on current security issues.

Securing computer data

Understanding the key principles of IT security

The security of IT systems is a necessary evil for many small businesses as it does take an amount of time and effort which many would rather spend on developing their sales, marketing and product delivery.

The scale of IT security that you need to implement will depend on the type of business that you run. For small sole trader businesses the amount of time devoted to this task can be quite small. For larger businesses or those that deal in sensitive areas then more time and effort will need to be devoted to securing your IT systems.

What is data security?

Data security is a set of policies, procedures and tools designed to protect your data from unauthorised access whether inadvertent or malicious.

In addition to securing your data, you will need to protect it from loss or corruption. This is probably one of the biggest threats to small businesses – losing your data could loose you your business.

What do I need to secure my data against?

There are a number of threats to your business data, including:

- **Mistakes** - people can accidentally delete data or records. Mistakes can be made by everyone in the business, so don't think that anyone, including the principals, are immune!
- **Malware** - this includes viruses and other "malicious software" that can harm data and computer systems.
- **Theft** - unfortunately you may loose data if hardware is stolen or individuals take your data without your permission.
- **Deception** - there are many email scammers who try and obtain passwords and login details in an attempt to steal money from business or personal bank accounts.
- **ID Theft** - this is a growing concern as thieves will steal data that is business confidential and then try and obtain services in the name of your business.

Most small businesses in the UK make bad targets for hackers. If someone has the skills to be a hacker or a fraudster, it makes sense that they target prominent, large organisations that are likely to be most profitable and which have the most lines of attack.

Smaller businesses keep tight control of their finances, and employees tend to know each other well. This makes them more difficult to attack. There is also some security in numbers. For example, if you send sensitive data in an email, there's a relatively small risk that someone will:

- Pick that email from the millions circulating on the internet at any time.
- Recognise that the data is sensitive.
- Have the ability to do anything about it.

You are, however, likely to face automated attacks from viruses and other malware since they attack very large numbers of businesses simultaneously and indiscriminately. The broad message is therefore:

- Doing nothing is unlikely to be an option for you; there are few businesses that would not suffer in some way if an attack on their data were to succeed.

- Take a measured approach. Security is a matter of finding a suitable balance between risk and inconvenience.
- Look for simple and effective ways to secure your data. Complexity brings its own risks. Simple provisions are the easiest to implement and maintain.

Please note

If you:

- hold a large amount of sensitive data
- hold data that might be particularly valuable to others
- are an obvious target for attack
- have reason to believe you might be singled out

We recommend that you seek the help of a suitable IT security consultant.

Security is always a balance

Data security is always a balance between the need to protect data and the need to operate as a small business.

You can have too much security. Taken to an extreme, security measures make it difficult for people to work. They can obstruct your clients, customers, suppliers and third parties that need to work with you.

You can have too little security. Everyone is under attack from automated tools that are constantly probing for weaknesses in your set up. Implementing simple, effective security does not cost a lot – it might cost you nothing at all.

There are few absolutes. Finding a suitable balance is not always easy, but it is something every business has to do. We will try to help you with that.

It follows that you should avoid security consultants that are not prepared to understand your business needs. You are likely to get unworkable and expensive solutions. Equally, you should not take advice from people that are dismissive of security issues. If the way forward is unclear insist on having the options and issues explained to you in business terms.

Not all security measures are technical

Remember, not all security has to be technical. You can beat many security problems by simply using common sense.

You probably have a cheque signing procedure. If your cheque signatories know your business well, it is difficult for someone to get cheques fraudulently regardless of how good they are at hacking into your systems.

Protecting important data

Protecting business data

This Guide is designed to help you protect your data from unauthorised access and inadvertent corruption. It will help you to find out and list what of your business data needs securing. By going through this process you can hopefully make sure nothing is forgotten about.

Why bother with data protection?

There is a great deal of 'hype' surrounding security. As a result many people are driven by the latest scare story. Since the basics of data security tend not to make the news they are easily overlooked. A list of your needs gives you the best chance of capturing all your security requirements and allows you to:

- Take an overview of your needs and create a set of measures that get you the best balance of security and inconvenience.
- Show the list to others to get feedback as to whether there is anything missing.
- Create a useful document to review your security measures if there is a new threat.

It is important to put this process into perspective and don't let it come in the way of running your business. Deal with the threat proportionately and you will be fine. For the majority of small businesses the biggest threat to their data is a member of staff accidentally deleting or damaging a file.

Taking stock of your security needs

We suggest you think about your own business and the types of data and systems that could be vulnerable:

- **Databases and data collections** - most businesses will run a small database or data collection. Initially this data may be on a simple spreadsheet. Think where you store your customer and supplier data. What about payroll or other internal data that could be very sensitive if it fell into the wrong hands? Both the file and probably the directory where it is located should be secured with a password.

- **Email and contact data** - many small businesses could not survive with the constant flow of email traffic they have with customers and suppliers. This data is secured on a server or maybe an off site location if your email is managed by an external provider. If the data is on a server in your office this must be secured with full password protection. In some small businesses there is a lot of sensitive data that flows via email, so this will need to be secured. It is possible to secure emails when they are being sent to a recipient but for the vast majority of small businesses this level of security is probably not needed. The biggest risk you face would be members of staff having access to a director or owners PC and reading their email directly. This may happen if you leave your desk for any length of time. If you consider this an issue implement security on your PC so that you can "lock" the PC when you are away from it. That way only someone that knows the password can unlock the PC. Some operating systems will automatically "lock" a workstation after a predetermined period of inactivity – such as not using the mouse or keyboard for 5 minutes. This is a useful feature.

- **Offsite data** - data held outside your office is, potentially, your biggest headache. It started with the diskette and the laptop and now includes, portable disks, CDs, DVDs and even digital cameras. Taking data off site is a boon for productivity (and necessary for protecting data from loss) but is a security nightmare. For example, it is very easy for a salesperson to download a contract to their PDA so they can work with it on the move. Alternatively they may use a memory stick to easily transfer documents to their home PC. But suppose they mislay the device. What if they left it at one of your major customers? You may also need to consider people taking work laptops home and using them remotely – how can they guarantee the laptop will be secure? A robust IT security policy, backed up by regular reviews, is often the only way to actively manage this type of problem.

- **Access from the outside** - It is possible for someone to load software on your PC without you knowing about it and accessing your files. This risk is absolutely minimal for most small businesses if you install and run updated industry standard protective software on your PCs.

A method for assessing security for your business data

If you feel particularly at risk it is possible to carry out an assessment of your business data, using a simple spreadsheet.

We suggest you use a simple system to identify how important it is to your business to protect a given network, device or set of data. Here's a scheme you might want to adapt to your needs:

1. **Critically important** - If someone were to gain unauthorised access our business could be in jeopardy.

2. **Business critical** - If someone were to gain unauthorised access we could lose significant business or a substantial amount of money.

3. **Internal exposure** - If someone where to gain unauthorised access they could damage data and systems but we would be able to recover without significant effect on the people we deal with.

4. **Annoyance** - unauthorised access could cause problems and some embarrassment, but nothing significant.

Prioritising data in this way will help you decide which data security measures you need to implement first, and establish the balance you need to make between security and inconvenience. Make sure that you secure this spreadsheet!

Controlling access to data

Protecting your data from unauthorised access

Every business has data that needs to be secured. If you are running a business as a sole trader then you do not need to really worry about others seeing any confidential data. But what happens when you start to employ people who may have access to your PC?

Even if they are not employed to work on a computer they may decide to jump into your seat when you are out and have a browse around the internet or your laptop data, looking at your confidential information.

Steps to secure your data

The chances are you will already have most, if not all, the equipment and software you need to implement the security measures you decided on in the planning phase.

Unfortunately, we cannot provide specific guidance for how to do that here because security features vary widely between products, operating systems and even versions of the same operating systems.

It is therefore possible that you will need to find someone that can help you create your access controls. If you do, make sure that you allow time for them to:

- Show you or someone else in the business what they are doing.
- Document the security measures they have implemented.

Most access controls are simple to update once you know what needs to be done. In your documentation, make copies of key screens and make notes as you go along so you build up a small user manual that means you do not have to involve someone from outside every time you want to make a change.

As you implement each security measure you should test it is effective.

Security responsibilities

It can be difficult for businesses to decide how best to manage and implement security controls. In particular, who should hold high-level passwords that provide access to sensitive data?

It is clearly desirable that managers make the decisions about who should have access to what data.

It is also likely that managers will not be able or willing to implement those decisions and will want to delegate that job to a relatively junior administrator. However, what is to prevent that administrator using their privileges to gain access to data they are, themselves, not authorised to see? If that person leaves the company, what is to prevent them creating holes in the security measures that they can exploit later on?

This is obviously not an issue in smaller businesses where the chief focus is on preventing external access to data or where you can place a high level of trust in your administrator.

If you are concerned about the access available to an administrator, we suggest you consider:

- Giving the business owner or a senior manager responsibility for changing high-level passwords once they have been created. Those passwords should be kept in a secured place readily available in case of emergency. If the passwords are needed, then either:

  - the appointed manager can enter the password; or

  - if they are not available, the password can be accessed and a new one can be created later on.

- Making sure anyone with sensitive data that needs to be withheld from the administrator knows how to encrypt that data with a personal password.

- If there is any concern about the circumstances in which an administrator leaves the business, ask a security consultant to:

  - Look for possible security holes.

  - Make sure all key passwords are changed.

  - Ensure that the business is not locked out from any data or systems.

- Implement some type of separation of duties, if appropriate. This is the principle of preventing one person having control of the data as well as the data security. For example you may have a database administrator who has complete access to your business data. By implementing separation of duties they will not be able to view the data they are backing up as their role is separate to the security role. This can be a difficult process to implement by may be beneficial if you deal with sensitive data.

Assigning data access rights

How to protect your data

This guide is designed to help you protect your data from unauthorised access and inadvertent corruption. Stopping people accessing your data is the best way of protecting it - prevention being better than cure.

There are some straight forward steps you can take to protect your data, none of which need you to be an expert in IT.

Please note: If you are supplying services to some companies or government agencies it may be a requirement of your contract that you can adequately protect and manage your systems, irrespective of the size of your business. In this case it is strongly suggested that you get the help of an experienced IT professional able to secure your data.

For further details on this look at the following guide:

Choosing an IT consultancy supplier (**www.businessitguide.com/guides/view-guide/11/**)

Understanding the threat

You need to understand what data you have and what needs to be protected. In reality many small businesses probably have a few spreadsheets and documents that need to be actively protected. Most of your other documents might still be private but not require such a high level of protection.

Key documents and data that will need protecting will probably be:

- Salary details
- Customer lists
- Bank details and online banking logons
- Passwords
- Intellectual property. If you produce files and documents which are then sold such as designs, schematics and plans these will need to be actively secured

Part of understanding the threat also needs you to think through who is likely to want to access or obtain this data. For most small businesses the risk of targeted theft or damage is low. Most damage would be as a result of mistakes such as accidental deletion or people not thinking through what they are doing.

If you feel that you may be at high risk of data loss it may be a worthwhile exercise to create a spreadsheet of your important files and understand the scope/nature of the problem. Make sure this spreadsheet is secured though! For many businesses this is an unnecessary task.

Granting access to your data

Access controls will usually need you to provide a user name or user id and password before you can get to the data. The computer system will validate that the user is entitled to have access to the data and they are who they say they are by providing a valid password.

There are different levels of protection you may decide to implement:

- **Computer-level protection**. This prevents people from accessing a computer (including servers, PCs and laptops) unless they have a valid user id and password. This level of security is effective against both external and internal attacks although people with physical access to a computer can by-pass this protection. You should consider this to be the minimum level of access control on all your computers. Locking a computer in a secure room is often the best way of protecting your data from casual access.

- **Folder-level protection**. You can allow/deny access to data based on the folder the data is stored in. For example, you might have a folder called 'Business plans' that is available to just one or two people. This protection is effective for collections of documents because you do not need to define security for each new document. You can also specify that new folders and files have the same security as the parent folders that hold them. This is normally a feature of the computer operating system, such as Microsoft Windows.

- **File-level protection**. You can allow/deny access to individual files. This is not used often because it takes more time and effort than folder-level protection, but it might be useful if you have just one or two files in a database folder that need to be protected.

There are three basic access restrictions that you can create for folders and files:

- **No access** – people cannot open the folder or file unless they have a valid id and password.

- **Read-only access** – people can see the file and can open it but can't change anything. That might be useful for documents that you don't want people to change such as health and safety regulations.

- **All access (often called read/write access)** – people can see, use and update the files.

All versions of Microsoft Windows and most other computer operating systems allow you to share folders across a network. It is easy to use these systems to create shared folders available to anyone connecting to your network.

We discuss this in more detail in Sharing Data (**www.businessitguide.com/guides/view-guide/33/**).

Tip: Keep it locked: 5 tips to ensure the security of your Windows PC

- Be wary about opening attachments, even from people that you know. If possible, have the attachment scanned first before opening it.

- Here are three applications that you need to install if you don't have them: an antivirus, an anti-spyware, and a firewall. All three are freely available from the Internet. Be sure to update them regularly.

- Avoid browsing websites with which you are not familiar and remember that potentially risk websites mainly come through forwarded emails.

- If you are using operating systems that predate Windows XP, you must frequently update and apply patches to your computer system. Choose the Windows option in your Start menu to get regular updates.

- Stay legal: avoid downloading illegal software applications or trying to crack them using patches available online. A large number of these software programmes contain hidden malware.

Computer viruses and malware

Protecting my business data from damaging software

It is an unfortunate fact of life that every networked computer is a potential victim of computer viruses and malware. If your computer is ever infected then it can result in catastrophic loss of important business data. Protecting this data and your PC equipment is therefore a vital part of running a small business.

This guide is designed to assist you in understanding the problems of malware and computer viruses and to give you some tips to help secure your computer equipment.

What is malware?

Across the world there are many hundreds of individuals who spend their time creating software that can damage computers. The term used to describe this software is “malware” and it encompasses all of the nasty software you may have heard of including viruses, Trojans, worms and adware. There are technical differences about the nature of such malware and indeed some is more damaging than others. Really you should not be concerned about these detailed differences, rather just focus on protecting your business computers from all malware.

A significant and rising concern is about malware called “BotNets”. This is software that is installed onto your PC without your knowledge and then takes over your computer such that it can become involved in sending out spam email messages or other malware. Some of these networks can comprise thousands of linked PCs, all controlled by a remote operator who steals your computer processing power. The only evidence of being infected is often just a slowing of your PC’s performance.

How to protect your business from Malware

First and foremost you need to ensure that you have purchased a product called antivirus software. This sits on each PC and makes sure that any damaging software is not allowed to enter the PC and cause problems. Because the nature of this malware threat changes regularly this software will rather cleverly download a new set of updated antivirus instructions every day to make sure you are keeping abreast of malware development.

Suppliers of anti-virus and anti-malware software

There are a large number of providers of antivirus software. Most of these products can be obtained on a subscription basis and may cost around £100 per year. Others may be available free of charge. Look for a supplier that has good widespread use as they will generally be up to date with the latest malware threats. To install the software you will normally visit the vendor’s website and then follow the instructions to set up on your PC. For suppliers that charge for the software you will need to enter registration details and a credit card number. Some computer hardware suppliers may sell you a new PC with a free trial subscription for some antivirus software. This is a useful service and worth taking advantage of, even if it only lasts for 60 days before you need to register.

Antivirus/malware suppliers include:

AVG UK - **http://www.avguk.com/doc/**

F-PROT - http://www.f-prot.com/

SOPHOS - **http://www.sophos.com/**

SYMANTEC - **http://www.symantec.com/index.htm**

LAVASOFT - **http://www.lavasoft.com/**

MICROSOFT - http://www.microsoft.com/athome/security/computer/default.mspx

MCAFEE - **http://www.mcafee.com/uk/**

Keeping your PC software up to date

Software manufacturers often need to make changes to their products to ensure they remain secure. This is in response to the hundreds of hackers that like to try and find a fault in the software and expose details such as passwords and banking details.

To prevent this happening you need to ensure that your business PCs are fully configured with these latest updates – sometimes referred to as patches. The good news is that most of the main stream business software vendors will automatically update your software for you – all you need to do is to “reboot”, or switch the computer off and then on again, for these changes to be implemented.

Most business users will use Microsoft software, and as such this is a large target for hackers to attack. It is strongly suggested that you take some time to visit the following Microsoft website and just make sure that you are receiving the latest updates for your Microsoft software, including Windows and Office.

The good news is that this is a free of charge service provided by **Microsoft** (**http://update.microsoft.com/microsoftupdate/v6/muoptdefault.aspx?returnurl=http://update.microsoft.com/microsoftupdate**).

Other steps you can take to keep your PC safe

Email is a vital tool for most businesses. Unfortunately it is also used as a mechanism to distribute malware. There are some steps you can take to further protect your business:

- Only open email attachments from people that you know.
- Only open email attachments when you have been told to expect one.
- Never click onto a website link contained in an email unless you can completely trust the sender of the message and the web site it is linking to.
- Never respond to “spam” email messages – it will lead you to being targeted by other spammers.
- Never respond to emails that appear to be from your bank requesting passwords.
- Don’t forward junk email, spam or “chain” emails – it wastes time and can make you a target.
- Be very careful which websites you visit – certain “unsavoury” websites can download malware without you knowing it.
- Never install software from a website unless you are 100% happy you trust the vendor or provider.
- Always check the website address (called a URL) and make sure it is correct – some hackers will alter the URL very slightly and redirect you to a rogue site.
- If in doubt – don’t!

Securing your data while travelling

Keeping Your data Secure on the Move

Most businesses rely on data. Even if you keep your customer list on a simple spreadsheet that data will be very important to you and your business. Imagine if that data was lost – think of the stress of trying to remember loads of customer names and prospects.

Like many things prevention is better than cure. This guide is designed to assist you understand the problems of loosing business data when you are out and about and provide you with some tips to help secure this important information.

How can business data go missing?

Think through your daily activities. Running a small business can mean dealing with a multitude of problems and issues, spending time visiting clients, prospects and suppliers. More and more business data is now sitting on PCs and hand held devices all of which are easy to loose or have damaged.

In a 6 month period over 63,000 mobile phones, 5,000 PDAs and 5,000 laptops were left in the back of London taxis alone!

Unfortunately portable electronic devices are also subject to the keen interest of the criminal fraternity and large numbers of devices are stolen from cars, airports, restaurants and anywhere else that people may put them down. The Friday evening wind down at the pub with the team may result in expensive kit being whisked from under your nose.

Electronic devices are also subject to damage. They are a lot tougher than they used to be, but dropping a laptop from a height of an average desk will pretty much destroy it and wreck the data on the hard drive. Laptops falling out of overhead bins on aircraft are also likely to get destroyed. The move to increased airport security has lead some airlines forcing laptops to be secured in the hold, not an ideal place for sensitive equipment.

Tips to stop your data being lost

Probably the best assumption to make before you travel with your PC is that the laptop will go missing or be damaged at some point on the trip. This should focus the mind and ensure that you back up or make a copy of the important data on the laptop. These small USB pen drives are ideal for taking a quick copy of your data – but make sure that you leave it somewhere safe, maybe back at the office or at home. Placing the USB drive in the same bag as a laptop is not a good idea. Some people will simply place the drive into their pocket so it is with them at all times and kept separately from the laptop which is a good idea.

Don’t forget to take a full backup of your data at other times as well. Depending on the amount of travel you do it may be an idea to back up data to a CD drive once a week or once a month and then use a USB drive in between times for smaller backups.

When you are carrying your laptop why not put it into a secure bag that does not look like a conventional laptop holdall? Some of the branded bags from the computer vendors are very good, but shout out loud that you have an expensive laptop in the bag.

When you arrive at your destination and get your laptop out make sure you secure it using a laptop lock. This comprises a piece of armoured cable that attaches to the laptop with a lock and goes around a fixed object. It is a bit like a bicycle lock and pretty secure. That way if you leave your laptop briefly then it will hopefully be there on your return. Another tip is to always secure your laptop in your hotel room or hide it all together, out of harms way. Sticking it in the bag with the dirty washing is often a good hiding place! Locking devices can cost between £25.00 and £75.00 depending on what type of device you want.

If you are in the type of job that requires you to take a laptop to a harsh environment consider a “ruggedised” laptop. These are especially designed to withstand harsh conditions such as water and physical shocks. They are great if you work in the building or surveying trade or otherwise work outside. Rugged laptops can cost between £1000 and £3000.

It is possible to secure data on a laptop by encrypting it. Once encrypted if the laptop goes missing at least your data should be secure. Some of these solutions are quite sophisticated and enable you to share data with trusted colleagues by providing keys to unlock the data. It’s a bit like issuing a set of keys to your office to trusted employees. If someone does not have a key then they cannot access the data. This type of data security can range in price from £50 per laptop through to about £100.

Suppliers of security products for mobile workers

Here are some suppliers of laptop locking devices:

KENSINGTON - **http://uk.kensington.com/html/6838.html**

COMPUCLAMP - **http://www.compuclamp.com/**

Here are some suppliers of “rugged” laptops;

TOUGHBOOK - **http://www.toughbook-europe.com/ENG/**

TERRALOGIC - **http://www.terralogic.co.uk/**

ITRONIX - **http://uk.itronix-europe.com/**

Here are some suppliers of data encryption products for laptop computers;

SECURITY MADE EASY - **http://www.security-made-easy.co.uk/**

PGP - **http://www.pgp.com/products/wholediskencryption/index.html**

DES - **http://www.des.co.uk/**

Tip: How to protect your data from prying eyes

- Delete temporary files when you finish working. Using a freeware application called **CCleaner (http://www.ccleaner.com/)** is very effective. Deleting temporary files (like the ones created by Word or your internet browser) not only safeguards your privacy, but also frees disk space helping improve computer performance.

- Encrypt your files, particularly those containing sensitive commercial information. Choose a password you will remember but other people will not guess. Avoid names of family members and “password”. Where possible use passwords with a combination of letters and numbers. One of the most powerful and popular encryption programmes is Phil Zimmermann's **PGP (http://www.pgpi.org/products/pgp/versions/freeware/)** which should protect your files from snoopers for some time.

- Protect your computer from sniffing applications like malware, key loggers and trojans, by installing security applications like a firewall, antivirus software and anti spyware. Some of the best ones are free to use.

- Prevent people from physically accessing your computer. Keep your computer in a secure location, use simple defences like a **Kensington lock (http://uk.kensington.com/html/6838.html)** on your laptop or desktop. Set a power-on or hard drive password and a log-in password to deter theft and snoopers.

- The simplest way to gather information from a computer is simply to look at the screen. To prevent people from “shoulder surfing” try covering your screen with a specially designed screen filter, or better still, work in a corner where you cannot be overlooked.

Ask our experts….

The following blogs were written by the Guide's top IT security experts and are based on their experiences of running their own businesses.

Laptop shoulder surfing - what you need to know (Steve Gold)

Laptops are now ubiquitous as a business tool, as a quick glance around coffee shops - with WiFi facilities, of course - trains and airport lounges will confirm.

But they are also a serious business espionage risk, as growing numbers of private detectives and allied agencies are shoulder surfing business travellers to extract useful business information.

The role of private detectives has changed immensely in recent years, largely thanks to the use of technology to help them achieve their often illegal aims.

You need information? Don't go to Pinkertons, as, whilst their labour-intensive activities produce results, technology can slice through the costs and time required to get the inside track on your competitors.

Well, that's the theory. 3M, which produces the Vikuiti range of screen and privacy filters, was at the Business Travel Show in London in early February, showing off its latest filters.

Nick Hughes, business development manager for 3M's optical systems division, said that stories of yet another security lapse by company X are hitting the headlines far too often.

They demonstrate, he says, just how vulnerable people are to threats such as privacy invasion, identity theft and fraud, and how little is being done to protect commercially sensitive on-screen data/

Hughes says that a privacy filter is a simple yet essential security gadget that offers a greater sense of comfort for anyone using their laptop during business travel - whether they are working in WiFi-friendly airports, a hotel lobby, on an airplane, bus or train.

According to IDC research dating from March of last year, there are now around 2.4 million laptop users at risk from prying eyes.

What's more, says Hughes, 3M's research suggests that eight out of 10 of these users may have already become victims of shoulder surfing.

As you might expect, Hughes advises laptop users to fit a privacy filter on their machines to allow an unrestricted view for the user but prevent others positioned to the side or viewing over their shoulder from seeing what is on the screen.

On a recent trip from London to Doncaster, I noticed several dozen people on the East Coast Main Line train using laptops - and the free WiFi service in both first and standard class.

The number of MS-Excel spreadsheets on display was significant.

Perhaps it's time to install a privacy filter after all.

Useful links: - **3M - http://www.3m.co.uk/privacyfilters**

Stopping your Data Escaping – (Mr BITG)

The amount of admin work I need to do is huge, in fact I seem to spend more time with my accountant sorting out the VAT than selling to new clients.

And then along comes another issue to worry about – keeping our data from trotting out the door with the latest disaffected salesperson to leave my team.

As a small business person I have been watching the news over the past few months with increasing amazement as organisation after organisation reveals stories of lost laptops, mislaid disks and nicked data.

What never ceases to surprise me is that most of these losses stem from people working inside the business. Forget burglars and robbers, we are talking about members of our own team that we interviewed and hired ourselves.

I’m not saying everyone is bad. Far from it.

But that is where the problem stems from. We have people that simply make mistakes, like putting disks of data in the post with out securing it or sending email messages to the wrong people. In fact in all my years in business I have only had a couple of sales people try and run off with data, and since then have certainly learnt my lesson.

So what am I doing to stop my data escaping?

First of all I am trying to set a good example by being careful with the business data myself. If I end up sending it out accidentally what kind of example does that give to my team? I took a look at the Business IT Guide and found a number of guides that give some pretty good basic tips about stopping my data going missing.

These included:

Controlling access to data **- http://www.businessitguide.com/guides/view-guide/23/**

Data security training **- http://www.businessitguide.com/guides/view-guide/22/**

Preventing hardware theft **- http://www.businessitguide.com/guides/view-guide/28/**

Protecting important data **- http://www.businessitguide.com/guides/view-guide/20/**

Securing computer data **- http://www.businessitguide.com/guides/view-guide/19/**

Keeping Laptop & PCs Safe and Secure **- http://www.businessitguide.com/guides/view-guide/27/**

Securing your data while traveling **- http://www.businessitguide.com/guides/view-guide/24/**

It’s surprising how simple some of these steps are, and after reading through the guides I realised that we had some holes in our security.

My two sales people both have laptops which they use for presentations and writing proposals. I had a look at one of them and saw how much confidential data was sitting on his unsecured laptop. We invested in some simple technology to protect this data so if the laptop was lost we could be certain it will still be secured. I also bought the guys a couple of those laptop locking cable gadgets so they could secure the laptop to a table when they were out and about.

Glossary

Data Protection Act - The Act that places legal requirements on businesses and individual agents to adequately protect and manage personal data. The Act now applies not only to data stored on a computer, but to any personal data you hold.

Encryption - The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key.

Network - Several different technologies allow computers to communicate with each other; when computers are connected this way, they are usually described as a 'network'.

Operating systems - Programming that boots automatically when you start a computer and provides you with the desktop and all of the facilities needed for applications such as word processing and your Internet browser.

USB (Universal Serial Bus) - Connection port on a computer that is universally compatible with many types of devices, such as printers, speakers and mice.

Viruses - Programs designed to exploit weaknesses in your security so as to replicate themselves between computers, usually causing damage as they go.